GOT SECURITY AWARENESS

May 2001

Introduction

Periodic Security Awareness Newsletters will be distributed to help GOT staff stay abreast of security-related issues. This newsletter focuses on Security Incident Reporting; User IDs and Passwords; Workstation Protection; Departing Staff Checklist; Badge Access and Internet and E-mail Acceptable Use Policies; the Kentucky Computer Crime Law, and Anti-Virus Tips. Further information is contained in the Security Policies and Procedures Manual (GOT-067) at www.gotsource.net/dscgi/ds.py/View/Collection-485. Also, the forms referenced in this newsletter can be found at http://www.gotsource.net/dscgi/ds.py/View/Collection-513.

Security Incident Reporting

It is the responsibility of all staff to report suspected security breaches to their branch manager by completing form GOT-F012. Security breaches can take many forms including:

- physical intrusions;
- electronic intrusions that include networks, servers, and workstations;
- incidents related to catastrophic disasters;
- breaches as a result of deception and/or fraud;
- loss or misplacement of media; and
- damage to equipment, facilities, or utilities, etc.

INSIDE THIS ISSUE

Workstation Protection

Properly safeguarding your PC is one of the most important ways to protect information from corruption or loss. The following steps are required:

1. If workstations are connected to a network and are not performing specialized approved background functions such as monitoring or logging, when unattended for an extended period of time, they must always be logged off. For specialized workstations that cannot be logged off, measures such as screensavers or physical security access to keyboards must be employed. Computers should be shut down when the user goes home for the day. (A computer that is logged on and locked can give the controller of a remote control trojan the logged-in user's access rights.)
2. Workstations (including laptops and notebook computers) must employ the approved McAfee virus screening programs at all times. Check with your LAN Administrator about how best to do this.
3. Laptops are high theft items. If you use a laptop, store it in a locked area when not in use--if your laptop is gone, so is your data. Backup your data whenever possible.
4. Only Commonwealth of Kentucky authorized applications and utilities may be loaded on user workstations.
5. For workstations that employ operating systems software that have the capability to enact password restrictions, such as Microsoft Windows NT, those capabilities must be configured and enabled.
6. Workstations with modems are not permitted unless previously approved by department management and the Division of Security Services. For those workstations authorized to have modems, auto-answer should be off.
7. When possible, remove your data before allowing your workstation to be repaired off-site or replaced by an outside vendor. Ask your LAN Administrator about how best to do this.

Internet/E-Mail Policy

Highlights of the Enterprise Policy for Internet and E-mail Acceptable Use follow. To see the entire policy, visit http://www.state.ky.us/got/policies/got_060.pdf.

GOT staff are encouraged to use the Internet and e-mail to accomplish job responsibilities more effectively and to enrich their performance skills. The Internet and e-mail afford unprecedented opportunities for conducting research and disseminating (publishing) job-related information.

The acceptable use of Internet and e-mail represents the management of a state business resource. Supervisors should work with employees to determine the appropriateness of using the Internet and e-mail for professional activities and career development during working hours, while insuring that employees do not violate the general provisions which prohibit using the Internet and e-mail for personal gain. However, excessive personal use of the Commonwealth's e-mail or Internet resources shall lead to loss of privilege to use them.

Employee Responsibilities:

Commonwealth of Kentucky staff members have an obligation to use their access to the Internet and e-mail in a responsible and informed way, conforming to network etiquette, customs, courtesies, and any or all applicable laws or regulations.

As with other forms of publications, copyright restrictions/regulations shall be observed.

GOT staff shall be aware that their conduct or information they publish could reflect on the reputation of the Commonwealth.

Use of Commonwealth of Kentucky Internet and e-mail resources is a privilege that may be revoked at any time for inappropriate conduct. Examples include:

- using the Internet for personal gain or illegal purposes;
- transmitting offensive or abusive language;
- knowingly visiting pornographic or illegal sites;
- misrepresentation of oneself or the Commonwealth;
- sending chain letters; and
- other activities that will cause congestion and disruption of networks and systems.

Badge Access Policy

In trying to establish adequate physical access and environmental controls, the following steps must be taken:

GOT staff must have a valid GOT security badge that authorizes access to GOT controlled areas, and it must be displayed at all times.

To obtain a badge or change access, form GOT-F019 must be completed by the immediate supervisor. The form requires information such as staff name, starting date of employment, signature of immediate supervisor, and primary building location, as well as any additional areas for which the staff needs access.

The Division of Security Services (DSS) should be contacted to schedule an appointment for a photo/badge. The completed GOT-F019 should be brought to DSS at 101 Cold Harbor Drive, or sent in PDF format via e-mail or faxed at 502/564-6856 prior to the appointment.

In the event of termination, it is the responsibility of the immediate supervisor to notify the DSS in order to disable the badge, and also to recover the badge, if at all possible (see "Departing Staff Checklist" below).

Departing Staff Checklist

When a staff member transfers, resigns, or has their employment terminated, the branch manager (or above) is responsible for initiating GOT-F042, "Departing Employee Checklist" which can be found at https://kyeasupt1.state.ky.us/gotexit/search.asp, and submitting it to the Division of Security Services (DSS) and Office of Human Resources Management and Development. The DSS will notify the building systems administrator, ensure that the security and parking badges are turned in, user IDs and passwords are revoked, appropriate accounts and directories are disabled or deleted, access privileges are removed, etc. For situations involving termination, the DSS must be notified **immediately** so user IDs assigned to the individual may be disabled. Additional review items for the branch manager/supervisor include:

Letter of resignation/employee evaluation status;
Subscriptions cancelled;
Telephone/Telephone Card/Pager;
Gasoline Card;
Security Badge Card; and
All equipment/software/reference materials/office supplies for which staff is responsible have been accounted for, as well as keys for filing cabinets, etc.

User IDs/Passwords

Passwords must be:

- Eight or more characters (password length for servers such as Windows NT, Unix, and Novell should be a minimum of 11 characters, whereas mainframe passwords are limited to 8 characters);
- Kept confidential;
- Encrypted when held in storage or when transmitted across the network when the path is connected to an external network;
- Mixed-case alphabetic or include non-alphabetic characters; and
- Changed at least every 31 days unless otherwise approved (non-expiring passwords must be approved on an exception basis). To change the password, hold and press Control/Alt/Delete to display the Windows NT Security Dialog Box. Press “change password.”

Passwords must not be:

- Reused or shared with others;
- Repeated sequences of letters or numbers;
- A word contained in English or foreign language dictionaries;
- Included in a macro or function key to automate the login;
- Stored in any file, program, command list, procedure, macro, or script where it is susceptible to disclosure or use by anyone other than the owner;
- Names of person, places, or things that are easily identified with the user;
- The same as the userid; and
- Displayed during the entry process.

GOT network domain passwords (findisnt) will be reviewed on a periodic basis, and all exceptions will be identified for those passwords that do not meet the guidelines.

Password Tips

These tips may help users to invent techniques of their own. Just using a technique of some sort improves one's ability to memorize a password.

In conjunction with using the following password creation tips, it is important to remember that all passwords should contain a special symbol (e.g., "#", "$", "@" or whatever special characters the system permits) in the first five characters, unless the application or operating system does not allow the use of special characters. If special characters cannot be used, then a combination of upper and lower case letters as well as numbers should be used.

1. Create a phonetic sentence using the pronounced sounds of the letters, numbers, or special characters.

   I10D-24GET "1 tend to forget."

   RU?LOSTIM "Are you lost I am!"

   187#2DAY? "I ate seven pounds today."

2. Concatenate short, unrelated words with symbols.

   GO$CATSAY BEES&PAWS

   W1N>TER60OF AND%BLACK13

   GRAY*POUR CAT#2HAT

3. Use the first letter of each word in a poem or song until you have enough letters (e.g., at least six).

   JAJ^WUTH "Jack and Jill went up the hill"

   HINS.NJA "Help! I need somebody. Not just anybody"

4. Mirror a word (in either direction); repeat process or truncate letters as needed to get appropriate length.

   GUST-TSUG FL@AREERA

   BOY!YOB!BOY FILLOLLIF

5. Use every other letter in phrase until you have enough letters.

   NW[S]HTMFR "Now is the time for all..."

   TB:ONTOEH "To be or not to be, that..."

6. Take someone else's full name that you can easily remember. Divide it into segments or blocks of the length you need for your password. You may rotate back through the name again if you need additional letters or truncate any extra letters. Drop the first block. Use any other block that is not an exact match for a proper name or word.

   "John Quincy Adams" JOHNQULN (Drop) CY-ADAMS-J (Keep)

   "Alexander Graham Bell" ALEXANDE (Drop) ER&GRAHAM (Keep)

7. Take a word from the dictionary that is long enough to qualify as a password. Replace some or all of the vowels with numbers or special characters (e.g., "#", "$", "@", or special characters the system permits in passwords).

   Mornings MRNGS

   Psychotic PS#CH#T#C

   Beancounter BENCONT$R

8. This one creates difficult passwords. Using the telephone keypad (but assigning "Q" and "T” to the number "I") as shown, choose a number you can easily remember and translate it into letters. If your number includes a zero, just keep the "0" as the character for your password. You will note that for each number (except zero) you will have at least two letter choices.

   1234#5678 QADI#LORT or ZBEH#KNRU

   24*689753 CI*MUXRLE or AG*MTWPJD

   100#78699 Z00#STOVVY or QO0#RUNXX

9. Take a word from the dictionary (or a proper name you like) that is long enough to qualify as a password. Put all of the vowels together and all of the consonants together.

   Friends IE:FRNDS Douglas OUA&DGLS

Kentucky Computer Crime Law

As declared in KRS 434.845 and 434.850 the following standards apply to the Kentucky Computer Crime Law and must be adhered to:

1.0 Unlawful Access to a Computer in the First Degree

A person is guilty of unlawful access to a computer in the first degree when he knowingly and willfully, directly or indirectly, accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof for the purpose of:

Devising or executing any scheme or artifice to defraud; or

Obtaining money, property, or services for themselves or another by means of false or fraudulent pretenses, representations, or promises; or

Altering, damaging, destroying, or attempting to alter, damage, or destroy any computer, computer system, or computer network, or any computer software, program, or data.

1.1 Unlawful Access to a Computer in the Second Degree

A person is guilty of unlawful access to a computer in the second degree when he, without authorization, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof.

Unlawful access to a computer in the second degree is a Class A misdemeanor.

A person is guilty of misuse of computer information when he:

Receives, conceals, uses, or aids another in doing so, any proceeds of a violation of Section 1.0, Unlawful Access to a Computer in the First Degree.

Receives, conceals, uses, or aids another in doing so, any books, records, documents, property, financial instrument, computer software, computer program, or other material, property, or objects, to have been used or obtained in violation of Section 1.0, Unlawful Access to a Computer in the First Degree.

Misuse of computer information is a Class C felony.

McAfee Anti-Virus Tips

Do not open any files attached to an e-mail from an unknown, suspicious or untrustworthy source.

Do not open any files attached to an e-mail unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through e-mail. Better be safe than sorry and confirm that they really sent it.

Do not open any files attached to an e-mail if the subject line is questionable or unexpected. If the need to do so is there, always save the file to your hard drive before doing so.

Delete chain e-mails and junk e-mail. Do not forward or reply to any of them. These types of e-mail are considered spam, which is unsolicited, intrusive mail that clogs up the network.

Do not download any files from strangers.

Exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program checks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with McAfee's anti-virus software.

Update your anti-virus software regularly. Over 500 viruses are discovered each month, so you'll want to be protected. These updates should be at the least the product's virus signature files. You may also need to update the product's scanning engine as well.

Back up your files on a regular basis. If a virus destroys your files, at least you can replace them with your back-up copy. You should store your backup copy in a separate location from your work files, one that is preferably not on your computer.

When in doubt, **always err on the side of caution** and do not open, download, or execute any files or e-mail attachments. Not executing is the more important of these caveats. Check with your product vendors for updates which include those for your operating system web browser, and e-mail. One example is Microsoft's security site at www.microsoft.com/security.

If you are in doubt about any potential virus related situation you find yourself in, contact your LAN administrator.